UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/664,992	09/18/2000	Teruyoshi Komuro	SONY-50L2204CON	5771

7590 05/19/2005

Wagner Murabito & Hao
Two North Market Street
Third Floor
San Jose, CA 95113

EXAMINER
TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/664,992	**Applicant(s)** KOMURO ET AL.	
	Examiner Thanhnga B. Truong	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _07/06/2004 (Amendment)_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-20_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-20_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _06 July 2004_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending.

2. In response to the applicant's request for reconsideration of the previous office action, the new ground of rejection is rendered below.

Double Patenting

3. Examiner acknowledges a terminal disclaimer has been submitted by the applicant on July 06, 2004.

Drawings

4. Figure 1 filed on July 06, 2004 is now accepted.

Specification

5. The abstract of the disclosure filed on July 06, 2004 is now accepted.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-3, 6-10, and 14-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Park (US 6,028, 932), and further in view of Matsuzaki (US 6,058,476).

a. Referring to claim 1:

i. Park teaches:

(1) a source device **[i.e., Figure 5 show the parallel data received at the interface portion and daisy chained down to the recording portion 8, this path is "a source device"]** for encoding an encryption mode identifier (EMI) code into an information packet and for transmitting said information packet over a communication interface, said source device comprising:

(a) a first encryption circuit for encrypting data of said information packet provided said EMI code indicates a first mode; and a second encryption circuit for encrypting said data of said information packet provided said EMI code indicates a second mode **[i.e., referring to Figure 5, an encrypting portion 7 for encrypting the output of copy prevention information correcting portion 6 (column 4, lines 4-6)]**; and

(2) a sink device for receiving said information packet from said communication interface, said sink device comprising:

(a) an extractor circuit for extracting said EMI code from said information packet **[i.e., As shown in FIG. 6, copy prevention information detecting portion 5 included a PES header detecting portion 10 for searching the parallel data in synchronization with a clock clk to detect the PES header, and a copy prevention information extractor 20, that is for "extracting said EMI code from said information packet", enabled by the PES header signal of PES header detecting portion 10 to detect the copy prevention information field (column 4, lines 8-14)]**; and

(b) a second decryption circuit (or decrypting portion) for decrypting said data of said information packet in response to said extractor circuit indicating that said EMI code is of said second mode **[i.e., referring to Figure 5, a decrypting portion 3 for decrypting the output of key inserting portion 2 and transmitting it as parallel data (column 3, lines 62-64)]**; and

(3) wherein said first mode is a copy prohibition mode indicating that said information packet is not to be reproduced by said sink device and wherein said second mode is a copy once inhibition mode indicating that said information packet is not to be reproduced more than once by said sink device **[i.e., First, when a mode of "No Copy" is detected from the additional copy information field of the PES header, VCR B is not able to enter its recording mode. Second, when a mode of "Copy Permitted" is detected in order to implement a copy prevention such as DAT mode, VCR B records but "No Copy" mode is recorded in the additional copy information field to interrupt recopying from a copying tape. This means that a secondary source tape may be formed from the original tape, the first source, but a third source tape cannot (column 5, lines 11-20)].**

ii. Although Park discloses the encryption portion 7 and decryption portion 3 in Figure 5, Park does not explicitly show in detail that the encryption portion 7 and decryption portion 3 each could perform two different functions for encryption and/or decryption. On the other hand, Matsuzaki teaches:

(1) Here, the encryption performed by the first encryption unit and the encryption performed by the second encryption unit may use the same conversion algorithm. With the above construction, the first encryption unit and the decryption unit can be combined into one converter, so the circuit size of the encryption IC can be reduced. Here, the first encryption unit and the decryption unit may decrypt and encrypt using key data stored in advance inside the IC, wherein one part of the key data is stored in a mask ROM area inside the IC, and the other part is stored in a programmable ROM area inside the IC. With the above construction, the problems that occur when the authentication key is made up of only mask ROM, and the problems that occur when the authentication key is made up of only programmable ROM can be avoided. Here, each of the devices which conduct encrypted communication may authenticate the other device by performing communication based on a challenge/response-type authentication protocol, wherein each encryption apparatus may further include a decryption unit for decrypting encrypted combined data sent from the device in communication in response to the challenge data; a separation unit for separating decrypted combined data into a first separated data which corresponds to the response data and a remaining second separated data an authentication unit which judges whether or not the first random number matches the first separated data, and in the event of a match, authenticates the device in communication; a second encryption unit for encrypting the second separated data in the event of authentication; and a second transmission unit which transmits the encrypted second separated data to the device in communication as response data, wherein the data transfer key generation unit generates the data transfer key by combining the first random number and the second separated data, wherein the decryption unit, the separation unit, and the second encryption unit are implemented through circuits inside the IC **(column 7, lines 47-67 through column 8, lines 1-17 of Matsuzaki).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Matsuzaki into Park's invention for ensuring the security of communication between devices using only a small encryption IC **(column 5, lines 31-32 of Matsuzaki).**

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matsuzaki into Park's invention because the prior method of equipping a single PC with all the parts for mutual authentication, the distribution of the data transfer key, and the encryption makes the size of the IC very large, and leads to an increase in cost. Therefore, the object of Matsuzaki's invention is to provide a highly-secure encrypted communication system and is ideal for realization using a small encryption IC **(column 5, lines 22-25 and lines 42-44 of Matsuzaki).**

b. *Referring to claim 2:*

i. Park further teaches:

(1) wherein said sink device is a bit stream recording device and wherein said sink device further comprises a recording media for recording said information packet provided said EMI code is of said second mode and wherein said EMI code of said information packet is altered to said first mode by said sink device upon recording onto said recording media; **[i.e., there is provided a copy prevention apparatus for a digital video system including: a reproduction block for adding key information to a reproduced bit stream, and decrypting and transmitting it; and a recording block for searching key information of the bit stream transmitted from the reproduction block to extract copy prevention information, and encrypting and recording the bit stream according to the extracted copy prevention information. The reproduction block includes: reproduction means for reproducing data recorded on tape; key insertion means for adding key information to the bit stream of the reproduction means; and decryption means for decrypting the output of the key insertion means and transmitting it to a recording-side VCR (column 2, lines 60-67 through column 3, lines 1-6)].**

c. *Referring to claim3 :*

i. Park further teaches:

(1) wherein said sink device further comprises a first decryption circuit (or decrypting portion) for decrypting said data of said information packet in response to said extractor circuit indicating that said EMI code is of said first mode **[i.e., referring to Figure 5, a decrypting portion 3 for decrypting the output of key inserting portion 2 and transmitting it as parallel data (column 3, lines 62-64)].**

d. *Referring to claim 6:*

i. Park further teaches:

(1) wherein said information packet represents a portion of a digital audio/visual program **[i.e., when recording is carried out by the satellite receiver or high-definition TV decoder and compressed video data is encoded in encoder 101, it is converted into a packet form in packet processing portion 102 as shown in Figure 1. If the compressed audio data is encoded in audio encoder 103, it is converted into a packet form in packet processing portion 104 (column 1, lines 55-60)].**

e. *Referring to claim 7:*

i. Park further teaches:

(1) wherein said first encryption circuit, said second encryption circuit, said first decryption circuit and said second decryption circuit are coupled to receive a same cipher key **[i.e., referring to key distribution when a conventional block-cipher or stream cipher algorithm such as data encryption standard (DES) encrypts or decrypts only with a secret key (column 2, lines 1-3)].**

f. *Referring to claims 8, 15, and 16:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

g. *Referring to claims 9 and 17:*

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

h. *Referring to claim 10:*

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

i. *Referring to claim 14:*

i. Park further teaches:

(1) a first hash circuit for generating said first key based on a common key; and a second hash circuit for generating said second key based on said common key and wherein said common key is transferred between said sink device and said source device before said information packet is received by said sink device **[i.e., referring to Figure 3, "a first hash circuit" and "a second hash circuit" are considered to include in key supply portion 107].**

j. *Referring to claim 18:*

i. Park further teaches:

(1) wherein said step of said source device receiving an information packet having a copy protection mode includes the step of said source device translating said information packet having encoded CCI information to extract said copy protection mode **[i.e., referring to Figure 5, a copy prevention apparatus of the present invention comprises a reproducing portion 1 for reproducing data recorded on tape, a key inserting portion 2 for adding a tape header start code and key field at the front end of a bit stream of reproducing portion 1, a decrypting portion 3 for decrypting the output of key inserting portion 2 and transmitting it as parallel data, a key detecting/correcting portion 4 for detecting a key field from the parallel data transmitted from decrypting portion 3, a copy prevention information detecting portion 5 for detecting a PES header from the key field detected and extracting copy prevention information, a copy prevention information correcting portion 6 for correcting the output of copy prevention information detecting portion 5 if necessary, an encrypting portion 7 for encrypting the output of copy prevention information correcting portion 6, and a recording portion 8 for recording the output of encrypting portion 7 on tape (column 3, lines 58-67 through column 4, lines 1-8)].**

k. *Referring to claim 19:*

i. This claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

l. *Referring to claim 20:*

i. This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above; and

ii. Part further teaches:

(1) wherein said sink device is a bit stream recorder [i.e., and recording means, that is "a bit stream recorder", for recording the bit stream encrypted in the encrypting means (column 3, lines 15-16)].

8. Claims 1, 3-8, 10-13, 15-16, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamauchi et al (US 6,047,103), and further in view of Matsuzaki (US 6,058,476).

a. *Referring to claim 1:*

i. Yamauchi teaches:

(1) a source device **[i.e., the information processing apparatus shown in Figure 15 includes a disk reproduction drive 125, that is "a source device", as the data transmitting device and an AV signal processor 126 as the data receiving device (column 25, lines 33-36)]** for encoding an encryption mode identifier (EMI) code into an information packet and for transmitting said information packet over a communication interface, said source device comprising:

(a) a first encryption circuit for encrypting data of said information packet provided said EMI code indicates a first mode; and a second encryption circuit for encrypting said data of said information packet provided said EMI code indicates a second mode [i.e., referring to Figure 15, an encrypting section included in a disk reproduction drive 125, for converting the retrieved digital data into encrypted digital data, wherein the "a first encryption circuit" and "a second encryption circuit" are considered to include in this encrypting section (column 5, lines 60-61)]; and

(2) a sink device **[i.e., the information processing apparatus shown in FIG. 15 includes a disk reproduction drive 125 as the data**

transmitting device and an AV signal processor 126 as the data receiving device , that is "a sink device" (column 25, lines 33-36)] for receiving said information packet from said communication interface, said sink device comprising:

(a) an extractor circuit for extracting said EMI code from said information packet **[i.e., referring to Figure 15, a controller 128, that is an extractor for "extracting said EMI code from said information packet" (column 25, lines 60-65)]**; and

(b) a second decryption circuit (or decryption portion) for decrypting said data of said information packet in response to said extractor circuit indicating that said EMI code is of said second mode **[i.e., referring to Figure 15, a decrypting section included in an AV signal processor 126 for converting the encrypted digital data into decrypted digital data (column 6, lines 51-52)]**; and

(3) wherein said first mode is a copy prohibition mode indicating that said information packet is not to be reproduced by said sink device and wherein said second mode is a copy once inhibition mode indicating that said information packet is not to be reproduced more than once by said sink device **[i.e., The CGMS code "00" indicates that the copying is permitted, "10" indicates that one-generation copying is permitted, and "11" indicates that copying is prohibited (column 13, lines 45-48)].**

ii. Although Yamauchi discloses the encryption circuit (as shown in Figure 16) and decryption circuit (as shown in Figure 17), Yamauchi does not explicitly show in detail that each circuit could perform two different functions for encryption and/or decryption. On the other hand, Matsuzaki teaches:

(1) Here, the encryption performed by the first encryption unit and the encryption performed by the second encryption unit may use the same conversion algorithm. With the above construction, the first encryption unit and the decryption unit can be combined into one converter, so the circuit size of the encryption IC can be reduced. Here, the first encryption unit and the decryption unit may decrypt and encrypt using key data stored in advance inside the IC, wherein one part of the key data is stored in a mask ROM area inside the IC, and the other part is stored in a

programmable ROM area inside the IC. With the above construction, the problems that occur when the authentication key is made up of only mask ROM, and the problems that occur when the authentication key is made up of only programmable ROM can be avoided. Here, each of the devices which conduct encrypted communication may authenticate the other device by performing communication based on a challenge/response-type authentication protocol, wherein each encryption apparatus may further include a decryption unit for decrypting encrypted combined data sent from the device in communication in response to the challenge data; a separation unit for separating decrypted combined data into a first separated data which corresponds to the response data and a remaining second separated data an authentication unit which judges whether or not the first random number matches the first separated data, and in the event of a match, authenticates the device in communication; a second encryption unit for encrypting the second separated data in the event of authentication; and a second transmission unit which transmits the encrypted second separated data to the device in communication as response data, wherein the data transfer key generation unit generates the data transfer key by combining the first random number and the second separated data, wherein the decryption unit, the separation unit, and the second encryption unit are implemented through circuits inside the IC **(column 7, lines 47-67 through column 8, lines 1-17 of Matsuzaki).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Matsuzaki into Yamauchi's invention for ensuring the security of communication between devices using only a small encryption IC **(column 5, lines 31-32 of Matsuzaki).**

iv. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matsuzaki into Yamauchi's invention because the prior method of equipping a single PC with all the parts for mutual authentication, the distribution of the data transfer key, and the encryption makes the size of the IC very large, and leads to an increase in cost. Therefore, the object of Matsuzaki's invention is to provide a highly-secure encrypted

communication system and is ideal for realization using a small encryption IC **(column 5, lines 22-25 and lines 42-44 of Matsuzaki).**

b. *Referring to claim3 :*

i. Yamauchi further teaches:

(1) wherein said sink device further comprises a first decryption circuit (or decryption portion) for decrypting said data of said information packet in response to said extractor circuit indicating that said EMI code is of said first mode **[i.e., referring to Figure 15, a decrypting section included in an AV signal processor 126 for converting the encrypted digital data into decrypted digital data (column 6, lines 51-52)].**

c. *Referring to claim 4:*

i. Yamauchi further teaches:

(1) wherein said communication interface is a serial communication interface conforming to the IEEE 1394 communication standard and wherein said information packet is a digital information packet **[i.e., As the digital interface, the SCSI was used in Examples 1 and 3 and the ATAPI was used in Example 2. Other interfaces may also be used as long as they can transmit AV digital data and connect a plurality of devices. For example, a digital interface defined in the IEEE P1394 may be used (column 42, lines 32-36)].**

d. *Referring to claim 5:*

i. Yamauchi further teaches:

(1) wherein said source device is a broadcast receiver device and further comprises a receiver circuit for receiving an information packet encoded with CCI information and for extracting a copy protection code therefrom and wherein said sink device is unable to process an information packet encoded with CCI information **[i.e., referring to Figure 15, a disk reproduction drive 125, that is "a source device" which is considered to be "a broadcast receiver device"].**

e. *Referring to claim 6:*

i. Yamauchi further teaches:

(1) wherein said information packet represents a portion of a digital audio/visual program **[i.e., the digital data received by the MPEG decoder 606 is subjected to a predetermined process and converted into a digital video signal and a digital audio signal. The digital video signal is output to the video signal processor 48. The digital audio signal is converted into an analog audio signal by the D/A conversion circuit 607 and audibly output via a speaker 47S (column 20, lines 3-9)].**

f. *Referring to claim 7:*

i. Yamauchi further teaches:

(1) wherein said first encryption circuit, said second encryption circuit, said first decryption circuit and said second decryption circuit are coupled to receive a same cipher key **[i.e., an encrypting function E(KEY1, DATA) encrypts data "DATA" with an encrypting key "KEY1". The encrypting function E(KEY1, DATA) has an inverse function, i.e., a decrypting function D(KEY2, DATA) where KEY2 denotes a decrypting key. That is, when EncryptData=E(KEY1, Data) where "EncryptData" denotes encrypted data, Data=D(KEY2, EncryptData) is satisfied. Accordingly, the original data "Data" can be obtained by operating the decrypting function D(KEY2, EncryptData) for the encrypted data "EncryptData" which has been encrypted by the encrypting function E(KEY1, Data). In this example, it is assumed that the encrypting key KEY1 in the encrypting function E is equal to the decrypting key KEY2 in the decrypting function D (i.e., "KEY1"="KEY2") (column 27, lines 34-46)].**

g. *Referring to claims 8, 15, and 16:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

h. *Referring to claim 10:*

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 4 above.

i. *Referring to claim 11:*

i. This claim has limitations that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 1 above.

j. *Referring to claim 12:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

k. *Referring to claim 13:*

i. This claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

l. *Referring to claim 18:*

i. Yamauchi further teaches:

(1) wherein said step of said source device receiving an information packet having a copy protection mode includes the step of said source device translating said information packet having encoded CCI information to extract said copy protection mode **[i.e., accordingly, in order to protect AV data at a high security level, the information processing apparatus of Example 2 is provided with components which encrypt and decrypt data, in addition to the mutual authentication between the data transmitting device and the data receiving device. With this configuration, since AV data has been encrypted, the copyright protection of AV data is ensured even if AV data on the I/O bus 122 is extracted by the controller 128 due to an erroneous operation (column 25, lines 57-65)].**

Response to Argument

9. Applicant's arguments filed July 06, 2004 have been fully considered and addressed at the above rejection.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

AU 2135

TBT
May 14, 2005